

METHOD FOR PREVENTING ILLEGITIMATE USE OF CHIP CARDS

5 Cross-Reference to Related Application:

This application is a continuation of copending International Application No. PCT/DE00/01544, filed May 16, 2000, which designated the United States.

10 Background of the Invention:

Field of the Invention:

The present invention relates to a method with which it is possible to detect whether an attempt is made at manipulatory intervention in a chip card or smart card.

Because chip cards should be reliable during regular use and, unauthorized use of the card must be detected, there is the problem that it is difficult to set a practical level of sensitivity for a system for protecting against attempts at intervention. A sensory protection system is intended to ensure that abnormal operating states that can be exploited during an attempt at intervention are sensed and attempts at manipulatory interventions are themselves detected. If the sensors are set at too sensitive a level so that they respond even when there are small deviations from the normal state, they also react to unavoidable small fluctuations in the

operating conditions. As a result, the reliability of the  
respective product is, under certain circumstances, greatly  
restricted, for example even slight short-term current  
fluctuations in a card reader lead to a reset of the  
5 controller. For this reason it is necessary to make  
compromises in the setting of the sensitivity of such  
protection sensors.

Summary of the Invention:

10 It is accordingly an object of the invention to provide a  
method for preventing illegitimate use of chip cards which  
overcomes the above-mentioned disadvantages of the prior art  
methods of this general type, in which an unauthorized attempt  
at intervention in a chip card can be reliably detected and  
15 prevented without the normal appropriate use of the card being  
adversely affected.

With the foregoing and other objects in view there is  
provided, in accordance with the invention, a method for  
20 detecting an attempt at manipulatory intervention in a smart  
card. The method includes the steps of using various sensors  
for detecting abnormal operating states; sensing an occurrence  
of an abnormal operating state by some of the sensors; and  
activating the sensors with a relatively high degree of  
25 sensitivity relative to an overall sensitivity of the sensors  
as a group after the abnormal operating state has been sensed.

In accordance with an added mode of the invention, there is the step of providing the sensors with different degrees of sensitivity and successively more sensitive sensors are  
5 activated after the abnormal operating state has been sensed.

In accordance with a further mode of the invention, there is the step of providing the sensors with sensitivities that can be set at different degrees, and the sensors that are used are  
10 successively switched to a higher sensitization state after the abnormal operating state has been sensed.

Other features which are considered as characteristic for the invention are set forth in the appended claims.

Although the invention is described herein as embodied in a method for preventing illegitimate use of chip cards, it is nevertheless not intended to be limited to the details described, since various modifications and structural changes  
20 may be made therein without departing from the spirit of the invention and within the scope and range of equivalents of the claims.

The construction and method of operation of the invention,  
25 however, together with additional objects and advantages

thereof will be best understood from the following description of specific embodiments.

Description of the Preferred Embodiment:

5 The method according to the invention provides for a stepped system for sensing an attempt at intervention in which sensors which are connected upstream do not immediately trigger a reset or a similar targeted countermeasure in every case, but rather only activate sensors which are connected downstream and which have a relatively high level of sensitivity. The  
10 problem of the restricted reliability is thus overcome because it is possible to react adequately even to small signals indicating an attempt at intervention. Such a multi-step sensor hierarchy can in particular also react in a targeted  
15 fashion to different signal combinations. It is possible, for example, for an optical sensor with a high level of sensitivity to activate electrical sensors which are connected downstream and have a relatively high level of sensitivity or to increase the sensitivity of such sensors.

20 The method according to the invention uses a sensor hierarchy with which it is possible to react indirectly to abnormal operating states. The sensors used are successively switched into a higher sensitization state and/or successively more  
25 sensitive sensors are activated. In this way, it is possible, in particular, also to bring about a situation in which

combinations of different signals indicating an attempt at intervention can be evaluated, for example optically and electrically or thermally. The method therefore permits a stepped reaction to scenarios in which intervention is attempted.

In principle, any desired combination of different sensors with different sensitivities can be used in the method according to the invention. For example, the accumulated occurrence of small spikes in the operating signals can be used to increase the sensitivity of the spike sensors, or it is possible to trigger an alarm indicating an attempt at intervention, and thus for example to trigger a reset, when there is a simultaneous occurrence of relatively small spikes in combination with an operating voltage which lies at the limit of the voltage sensors.